



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/785,242	02/24/2004	David Lee Motsinger	1503/6	1031
25297 7590 08/24/2007 JENKINS, WILSON, TAYLOR & HUNT, P. A. SUITE 1200, UNIVERSITY TOWER 3100 TOWER BOULEVARD DURHAM, NC 27707			EXAMINER KANE, CORDELIA P	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 08/24/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/785,242

Applicant(s)

MOTSINGER ET AL.

Examiner

Cordelia Kane

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 24 February 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-143 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-143 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 27 September 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 8/10/2004.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is responsive to the non-provisional application filed on February 24, 2004. Claims 1 – 143 are pending. Claims 1, 26, 49, 74, 99, and 119 are independent.

Information Disclosure Statement

2. The information disclosure statement filed August 10, 2004 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.
3. The information disclosure statement filed August 10, 2004 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

Drawings

4. The drawings were received on September 23, 2004. These drawings are accepted.

Specification

5. The disclosure is objected to because of the following informalities:
6. Remove "Description" before the title on the first page.
7. Include application serial numbers for the named applications in the paragraph "Related Applications" on the first page.
8. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Appropriate correction is required.

Claim Objections

9. Claims 12 and 60 are objected to because of the following informalities:
reference is made to step b as well as to associating the threat score. The threat score is not actually mentioned until step c.
10. Claims 15, 39, and 63 refer to an predetermined user. It should read a predetermined user.
11. Appropriate correction is required.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2132

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. Claims 1 – 16, 21, 23 – 40, 45 – 64, 69, 71 – 89, 95 – 112, 117 – 134, and 140 – 143 are rejected under 35 U.S.C. 102(b) as being anticipated by Guthrie et al's US

Patent 6,161,185. Referring to claims 1, 26 and 49, Guthrie teaches:

- a. Monitoring communications between a server and a client (column 4, lines 65-66).
- b. Applying at least one detector to the communication data to identify a predetermined activity (column 8, lines 7-10).
- c. Generating a threat score associated with the predetermined activity by comparing the identified activity with a security threshold criteria (column 8, lines 10-17).

14. Referring to claims 2, 27, and 50, Guthrie teaches generating an alert based on the threat score (column 9, lines 8-10).

15. Referring to claims 3, and 51, Guthrie teaches performing steps a-c transparent to the communication of data between the server and the client (column 2, lines 54-56).

16. Referring to claims 4, 28, and 52, Guthrie teaches that the network may be a local area network (column 5, lines 4-5).

17. Referring to claims 5, , 29, and 53, Guthrie teaches that the communication data comprises HTTP protocol (column 5, lines 3-4). While Guthrie does not specifically teach that HTTP is the application protocol, Guthrie does teach that the Internet is the Network so it is inherent that HTTP would be the protocol.

18. Referring to claims 6, 30, and 54, Guthrie teaches that communication data comprises HTTP requests from the client and HTTP responses from the server (column 14, lines 4-5). While Guthrie does not specifically teach HTTP requests and responses, Guthrie does teach that the server is a web server so it is inherent that there would be HTTP requests and responses.

19. Referring to claims 7, 31, and 55, Guthrie teaches that the server is a web server (column 14, lines 4-5).

20. Referring to claims 8, 32 and 56, Guthrie teaches that the client is enabled by a web-enabled device including a unique Internet protocol address (column 13, line 49).

21. Referring to claims 9, 33, and 57, Guthrie teaches that the communication data comprises TCP packets (column 5, lines 2-3). While Guthrie does not specifically teach that there are TCP packets, Guthrie does teach that it is a TCP/IP network and therefore TCP packets would be inherent.

22. Referring to claims 10, 11, 34, 35, 58 and 59, Guthrie teaches associating the activity with a login session wherein the server is provided at least a username and password (column 7, lines 16-19).

23. Referring to claims 12, 36, and 60, Guthrie teaches associating the threat score with the client (column 8, lines 7-10).

24. Referring to claims 13, 37, and 61, Guthrie teaches that the threat score is generated when the activity deviates a predetermined amount from the security threshold criteria (column 8, lines 14-17).

25. Referring to claims 14, 38, and 62, Guthrie teaches that the security threshold criteria is an expected activity for the client (column 7, lines 60-63). Requesting the SADB challenge, and sending the account ID is inherently expected to happen for the client.

26. Referring to claims 15, 39, and 63, Guthrie teaches that the detector identifies when the communications data from the client is associated with a predetermined user (column 7, lines 54-55).

27. Referring to claims 16, 40 and 64, Guthrie teaches that the predetermined activity is a login activity (column 8, lines 7-10).

28. Referring to claims 21, 45, and 69, Guthrie teaches that the at least one detector is a plurality of detectors (column 7, lines 54-55, and column 8, lines 7-10). There are more than one detectors. One for detecting when the user is a system administrator and one for detecting when there are too many successive login failures.

29. Referring to claims 23, 46, and 71, Guthrie teaches displaying the alert to the operator (column 8, lines 4-6).

30. Referring to claims 24, 47 and 72, Guthrie teaches displaying the threat score (column 9, lines 35-38).

31. Referring to claims 25, 48 and 73, Guthrie teaches providing a user interface for enabling an operator to configure the security threshold criteria (column 8, lines 38-40).

32. Referring to claims 74, 99, and 119, Guthrie teaches:

- d. Monitoring communications between a server and a client (column 4, lines 65-66).

Art Unit: 2132

- e. Applying a plurality of detectors to the communications data wherein each detector detects different predetermined activity (column 7, lines 54-55, column 8, lines 7-10, column 9, lines 22-24, 39-42).
 - f. Generating an individual threat score for each detector (column 7, line 55, column 8, lines 10-14, column 9, lines 32-35, 62-64).
 - g. Generating an overall threat score for the client by combining the individual threat scores (column 11, lines 11-17).
33. Referring to claims 75, 100, and 120, Guthrie teaches generating an alert based on the threat score (column 9, lines 8-10).
34. Referring to claims 76, and 121, Guthrie teaches performing steps a-d transparent to the communication of data between the server and the client (column 2, lines 54-56).
35. Referring to claims 77, 101, and 122, Guthrie teaches that the network may be a local area network (column 5, lines 4-5).
36. Referring to claims 78, 102, and 123, Guthrie teaches that the communication data comprises HTTP protocol (column 5, lines 3-4). While Guthrie does not specifically teach that HTTP is the application protocol, Guthrie does teach that the Internet is the Network so it is inherent that HTTP would be the protocol.
37. Referring to claims 79, 103, and 124, Guthrie teaches that communication data comprises HTTP requests from the client and HTTP responses from the server (column 14, lines 4-5). While Guthrie does not specifically teach HTTP requests and responses,

Art Unit: 2132

Guthrie does teach that the server is a web server so it is inherent that there would be HTTP requests and responses.

38. Referring to claims 80, 104, and 125, Guthrie teaches that the server is a web server (column 14, lines 4-5).

39. Referring to claims 81, 105 and 126, Guthrie teaches that the client is enabled by a web-enabled device including a unique Internet protocol address (column 13, line 49).

40. Referring to claims 82, 106, and 127, Guthrie teaches that the communication data comprises TCP packets (column 5, lines 2-3). While Guthrie does not specifically teach that there are TCP packets, Guthrie does teach that it is a TCP/IP network and therefor TCP packets would be inherent.

41. Referring to claims 83, 84, 107, 108, 128 and 129, Guthrie teaches associating the activity with a login session wherein the server is provided at least a username and password (column 7, lines 16-19).

42. Referring to claims 85 and 130, Guthrie teaches associating the threat score with the client (column 8, lines 7-10).

43. Referring to claims 86, 109, and 131, Guthrie teaches that the threat score is generated when the activity deviates a predetermined amount from the security threshold criteria (column 8, lines 14-17).

44. Referring to claims 87, 110, and 132, Guthrie teaches that the security threshold criteria is an expected activity for the client (column 7, lines 60-63). Requesting the SADB challenge, and sending the account ID is inherently expected to happen for the client.

45. Referring to claims 88, 111, and 133, Guthrie teaches that the detector identifies when the communications data from the client is associated with a predetermined user (column 7, lines 54-55).

46. Referring to claims 89, 112 and 134, Guthrie teaches that the predetermined activity is a login activity (column 8, lines 7-10).

Referring to claims 95, 96, 140 and 141, Guthrie teaches selectively generating an alert and displaying it to the operator based on the overall threat score (column 11, lines 11-17).

47. Referring to claims 97, 117, and 142, Guthrie teaches displaying the individual threat scores associated with the detectors (column 9, lines 32-38, column 10, lines 11-17).

48. Referring to claims 98, 118 and 143, Guthrie teaches providing a user interface for enabling an operator to configure the security threshold criteria (column 8, lines 38-40).

Claim Rejections - 35 USC § 103

49. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2132

50. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

51. Claims 17 – 20, 41 – 44, 65 – 68, 90 – 93, 113 – 116, and 135 – 138 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guthrie as applied to claims 1, 26, 49, 74, 99, and 119 above, and further in view of Ben-Itzhak's US Publication 2003/0204719 A1. Guthrie discloses all the limitations of the parent claim. Guthrie does not explicitly disclose wherein the activity is, form manipulation, session cookie manipulation, protocol activity, or URL encoding. However, Ben-Itzhak discloses:

- h. Form manipulation (page 2, paragraph 19).
- i. Session cookie manipulation (page 3, 23).
- j. Protocol Activity (page 3, paragraph 24).
- k. URL encoding (page 2, paragraph 14).

52. Guthrie and Ben-Itzhak are analogous art because they are from the same field of endeavor, network protection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Guthrie and Ben-Itzhak before him or her, to modify activity monitoring of Guthrie to include manipulation of forms, session cookies, protocol activities and URLs of Ben-Itzhak. The motivation for doing so would have been that conventional security solutions are unable to meet the

unique security needs of each component in a multi component system (page 2, paragraph 12). Therefore it would have been obvious to combine Ben-Itzhak with Guthrie to obtain the invention as specified in the instant claims.

53. Claims 22, 70, 94, and 139 rejected under 35 USC 103 (a) as being obvious over Guthrie in view of Jackson's US Publication 2002/0188864 A1. Guthrie discloses all the limitations of the parent claim. Guthrie does not explicitly disclose adding the threat scores to generate a total threat score. However, Jackson discloses using single activity ratings combined to produce an accurate rating for multiple activities (pages 3-4 paragraphs 38-40).

54. Guthrie and Jackson are analogous art because they are from the same field of endeavor, network protection. At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of Guthrie and Jackson before him or her, to modify Guthrie to include generating a total threat score of Jackson. The motivation for doing so would have been it is difficult to rate multiple activities occurring simultaneously (pages 3-4, paragraph 40). Therefore it would have been obvious to combine Jackson with Guthrie to obtain the invention as specified in the instant claims.

Conclusion

Art Unit: 2132


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Cordelia Kane whose telephone number is 571-272-7771. The examiner can normally be reached on Monday - Thursday 8:00 - 5:00 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CPK

Cordelia Kane
Patent Examiner
Art Unit 2132


Benjamin E. Lerner
Examiner Art Unit 2132